SECURITY

Sarbari Gupta, PhD, CISSP, CISA, is the Chief Executive Officer of Electrosoft Services, Inc. Dr. Gupta possesses extensive expertise in cybersecurity, risk management, privacy and cryptographic solutions. She is a prolific speaker and writer with 20+ technical papers/presentations in refereed conferences/journals. She has co-authored several NIST Special Publications in the areas of Electronic Authentication, Security Configuration Management and Mobile Credentials; contributed chapters to cybersecurity books; and published numerous articles high-tech magazines.

Protecting the user as a high-value asset to achieve a safer cyber world

May 27, 2022

Sarbari Gupta

Who is protecting the online user? The answer is no one.

In fact, most IT environments consider users to be liabilities, not assets deserving protection. They are seen as the weakest links in the cybersecurity protection scheme. Why? Users browse unsafe websites, open emails with embedded malware, or click on links in messages.

Organizations load endpoint protection tools onto end-user computers, such as anti-virus, anti-spam, anti-phishing and safe browsing. They mandate ongoing user training in security and privacy to aid in the system's protection. Yet, while they increasingly harden systems and networks, they overlook user protection. It is no wonder that users are increasingly viewed as soft targets for attacks.

The End-User Dilemma

Some may question, "What is the point of protecting users?" Upon careful consideration, they might come to a different conclusion.

Consider all the passwords and PINs to various systems that house data or services, including remote access to organizational systems that users possess. Think about all their personally identifiable information (e.g., date of birth, Social Security Number, mobile phone number, etc.). Contemplate the credit card and financial information that bad actors can use to steal virtual money — and actual money — through online schemes. It is little wonder that bad actors bombard end users with cyberattacks.

Because users interface with the cyber world on many levels, risk increases. Most people maintain multiple email accounts, use many downloaded apps, have multiple social media accounts, bank online, etc. They create many avenues through which requests for information or demands for action, immediate or otherwise, can appear.

Many users have fallen for an online attack at one time or the other. Even sophisticated IT users will find it difficult to discern clever phishing attacks or be unable to distinguish authentic website URLs from those that are one character off. Still, others might react too quickly to messages detailing a large sum debited from their bank account and click the link without thinking.

A Solution and Call to Action

So, what is the solution to this problem? It is time to focus our security protection mechanisms on the user. We must start considering users as not only the subjects of online transactions but also the objects of transactions initiated by other parties.

I propose creating a user centric zero trust (UC-ZT) solution. User centric puts the end user as the focus of the solution. Zero trust asserts a default position wherein users place no trust in any entity trying to interface with them.

Many technologies can help enable UC-ZT environments. For example, Secure Socket Layer) and TLS (Transport Layer Security) (SSL/TLS), Secure Secure/Multipurpose Internet Mail Extension (MIME) encrypted and signed email, bad URL scanning tools and more can play a role. However, they are neither robust nor easy to apply consistently. Plus, such technologies place great responsibility on users and their ability to discern and thwart attacks.

My call to action is straightforward: We need a new mindset within the cybersecurity community that recognizes the user as a high-value asset in need of multi-layered protection. To promote UC-ZT architectures, we need more focused research and development to strengthen existing technologies and identify new ones that offer robust protection across all channels.

For too long, we have tried to protect systems and data. Now, our collective talents must focus on approaching the problem from an additional perspective, recognizing that users, too, possess knowledge and capabilities that the bad actors desperately want.

A new cyber age is dawning. It offers cybersecurity professionals the opportunity to leverage the lessons learned in protecting networks, devices and data in the creation of novel solutions to protect end users. UC-ZT will heighten cybersecurity at a time when the world is experiencing ever more attacks.

Sarbari Gupta, PhD, CISSP, CISA, is the Chief Executive Officer of Electrosoft Services, Inc. Dr. Gupta possesses extensive expertise in cybersecurity, risk management, privacy and cryptographic solutions. She is a prolific speaker and writer with 20+ technical papers/presentations in refereed conferences/journals. She has co-authored several NIST Special Publications in the areas of Electronic Authentication, Security Configuration Management and Mobile Credentials; contributed chapters to cybersecurity books; and published numerous articles high-tech magazines.

Get our new eMagazine delivered to your inbox every month.

Stay in the know on the latest enterprise risk and security industry trends.

SUBSCRIBE TODAY!

Copyright ©2022. All Rights Reserved BNP Media.

Design, CMS, Hosting & Web Development :: ePublishing